

NETWORK INVESTIGATIONS TRACK

NIT301, Network Monitoring Course (NMC)

Who Should Attend

DCIO/DoD/Federal law enforcement agents and prospective intrusion analysts.

Prerequisites

TT110 (INCH), RT120 (CIRC), FT210 (WFE-E) or FT215 (WFE-FTK) and one of the following: IT250 (FISE), IT260 (FIWE) or IT270 (FILE)

Duration

5 Days

Course Description

NMC teaches how to strategically place a monitoring sensor onto a network to capture traffic to and from a specific host. Students learn how to evaluate a network, both physically and logically, to determine proper sensor placement. Students also learn how to filter network traffic to comply with wiretap authority, hide the presence of the monitoring workstation on the network, and evaluate captured traffic for the proper content.

Objectives

- Explain how to legally monitor traffic on a network
- Explain how to properly prepare for network monitoring
- Deploy a network monitoring AIS
- Configure Windows network monitoring AIS
- Configure Linux network monitoring AIS
- Analyze gathered data in a Windows environment

Topics Covered

Network Monitoring Preparation

- Identify the key components for establishing network monitoring
- Select personnel with the proper skill sets/traits and know training requirements
- Know facility design requirements and equipment needs

Windows Network Monitoring

- Configure Windows network monitor
- Install and configure software including Wireshark, CoolMiner, jpcap, tcpdump, Keystroke Loggers, and VNC
- Deploy Windows based network monitor
- Collect, analyze, and verify data

Linux Network Monitoring

- Configure Linux network monitor
- Install and configure software including Wireshark, jpcap, tcpdump, and Keystroke Loggers
- Deploy Linux based network monitor
- Collect, analyze, and verify data

NETWORK INVESTIGATIONS TRACK

Preparation

To prepare for this course, we recommend the following review, reading, or research:

- Review the *Introduction to Networks and Computer Hardware* (INCH), the *Computer Incident Responders Course* (CIRC), and any of the DCITA Intrusions Track (FISE, FILE, or FIWE) course books, paying special attention to:
 - INCH: Basic Linux commands; device naming; device mounting and vi; basic Windows navigation; drive lettering and DOS commands; basic networking knowledge such as physical and logical topologies, IP basics, and command line networking tools.
 - CIRC: Device mounting in Linux; internetworking dealing with network data flow; witness devices and collecting volatile data collection; IP/subnet basics.
 - FIWE/FILE/FISE: Log analysis, using Ethereal, and how to decipher binary traffic

NMC Grading Policy

Student progress is monitored through instructor observation during lecture, discussion and practical exercises as well as Knowledge and Performance Tests. Minimum passing score on all DCITA tests is 70%.